NOT VOTING—13

Bachmann	Kennedy	Rangel
Blackburn	Lynch	Shimkus
Gohmert	Markey	Westmoreland
Holding	Miller, Gary	
Hurt	Neal	

□ 1418

Mr. RAHALL, Ms. PELOSI, Ms. BROWNLEY of California, Mr. CÁRDENAS and Ms. WILSON of Florida changed their vote from ''yea'' to ''nay.''

Messrs. KING of New York, YOHO and AMASH changed their vote from ''nay'' to ''yea.''

So the resolution was agreed to.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

APPOINTMENT OF MEMBERS TO THE BOARD OF VISITORS TO THE UNITED STATES COAST GUARD ACADEMY

The SPEAKER pro tempore (Mr. RODNEY DAVIS of Illinois). The Chair announces the Speaker's appointment, pursuant to 14 U.S.C. 194, and the order of the House of January 3, 2013, of the following Members on the part of the House to the Board of Visitors to the United States Coast Guard Academy:

Mr. COBLE, North Carolina

Mr. COURTNEY, Connecticut

□ 1420

CYBER INTELLIGENCE SHARING AND PROTECTION ACT

GENERAL LEAVE

Mr. ROGERS of Michigan. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and include extraneous material on the bill H.R. 624.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Michigan?

There was no objection.

The SPEAKER pro tempore. Pursuant to House Resolution 164 and rule XVIII, the Chair declares the House in the Committee of the Whole House on the state of the Union for the consideration of the bill, H.R. 624.

The Chair appoints the gentlewoman from Florida (Ms. ROS-LEHTINEN) to preside over the Committee of the Whole.

□ 1422

IN THE COMMITTEE OF THE WHOLE

Accordingly, the House resolved itself into the Committee of the Whole House on the state of the Union for the consideration of the bill (H.R. 624) to provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and for other purposes, with Ms. ROS-LEHTINEN in the chair.

The Clerk read the title of the bill.

The CHAIR. Pursuant to the rule, the bill is considered read the first time.

The gentleman from Michigan (Mr. ROGERS) and the gentleman from Maryland (Mr. RUPPERSBERGER) each will control 30 minutes.

The Chair recognizes the gentleman from Michigan.

Mr. ROGERS of Michigan. I yield myself such time as I may consume.

I want to thank my ranking member and both the Republican and Democratic staffs and the Republican and Democratic members of the Intelligence Committee for 2 years of long hours in negotiated efforts to reach the point that we are.

I want to back up just a little bit and tell you how we got to where we are today. We sat down some 2 years ago when the ranking member and I assumed the leadership of the Intelligence Committee and we looked at the one threat that we knew existed but we were not prepared to handle as Americans, both the private sector and the government. And we knew that we had to do something about this new and growing and misunderstood cyber threat and what it was doing to our intellectual property across the country, what it was doing to the freedom and open Internet that we so enjoy and are increasingly dependent on and the commercial value of our growing economy. And it was at risk. The private sector was at risk because people were stealing their identities, their accounts, their intellectual property, and subsequent to that, their jobs, and people began to question the value of getting on the Internet and using it for commercial purposes. Their trust in the free and open Internet the way we've embraced it in the United States really was at risk.

How do we solve that problem? We knew that nation states were investing millions and billions of dollars to generate cyber warriors to go in and crack your computer network. I don't care if you had intellectual property—those blueprints that made your business successful, or maybe it was your bank account, or your ability to have a transaction. If they could interrupt that, they could do great harm to our economy and to the United States.

We saw nation-states like Russia and China and now Iran and North Korea and others developing military-style attacks to actually do harm to the U.S. economy, to hurt the very men and women who get up every day and play by the rules and think that the Internet would be a safe place for them to interact when it comes to commerce. We want that to continue.

So we sat down and we talked to industry folks, people who are in the business, high-tech industry folks from Silicon Valley, financial services folks from New York City, manufacturers from across the Midwest, who were losing intellectual property due to theft from nation-states like China. We talked to privacy groups. We talked to the executive branch. And over the last 2 years, there were some 19 adjustments to this bill on privacy.

We believe this: this bill will not work if Americans don't have confidence that it will protect your privacy and civil liberties while allowing one very simple thing to happen: cyber threat material, that malware that goes on your computer and does bad things, allows somebody else to take over your computer to attack a bank, allows them to go on your computer and steal your personally identifiable information and use it in a crime, allows them to go into your network at work and steal your most valuable company secrets that keep you alive and build great products here in the United States—could we allow the government to share what they know with the private sector and allow the private sector to share when it comes to just that cyber threat, those zeros and ones in a pattern that equates to malicious code traveling at hundreds of millions of times a second the speed of light, can we share that in a way to stop them from getting in and stealing your private information?

And the good news is the answer is, yes, we can do this. We can protect privacy and civil liberties, and we can allow this sharing arrangement, but not of your identity, not of your personally identifiable information. As a matter of fact, if that's what's happening, it won't work. But at the speed of light, from machine to machine, from your Internet service provider before it ever gets into your network they bounce out the nastiest stuff that's in there that's going to take over your computer, steal your money, steal your personally identifiable information, steal your company secrets. And they can identify that by a pattern and kick it out. They'll say, Something looks bad about that. Can the government take a look at that and say, you know what? This is a Chinese attack, it's an Iranian attack, it's a North Korean attack—let's defend our networks. It's really very simple.

Today, what you see is a collaborative effort. This isn't a bill by DUTCH RUPPERSBERGER and MIKE ROGERS and this is the only way it has to be. We have taken suggestions from all the groups I just talked about, from privacy to the executive branch to industry to other trade associations. And this is the bill that mutually all of those people, representing tens of millions of employees around this country, said this is the way you do this and protect the free and open Internet and you protect civil liberties. And you finally raise that big red sign that tells people like China and Iran and Russia, stop. We're going to prevent you from stealing America's prosperity.

I heard a lot of debate earlier on the rule. I've heard a lot of misinformation. There are people who don't like it for whatever reason, maybe it's conviction, maybe it's politics, maybe it's political theater. And I have a feeling there's a little bit of all of that when they talk about this bill.

This bill does none of the things I've heard talked about in the rule—that